Computer and Internet Security Report

Monthly Update

March 1, 2020

Contents

About this Document **3**

Security News Digest **4**

Lock down your Gmail account like it's Fort Knox with the Google Advanced Protection Program 4

Iranian Phishers Use Journalist's Identity to Steal Info by Offering an Interview 4

Iranian hackers have been hacking VPN servers to plant backdoors in companies around the world 5

90% of UK Data Breaches Due to Human Error in 2019 5

Bezos, WhatsApp Cyberattacks Show Growing Mobile Sophistication 6

Microsoft Leaves 250M Customer Service Records Open to the Web 7

Microsoft says it now will continue to support Security Essentials for Windows 7 8

You can still get Windows 7 updates without paying a penny to Microsoft 8

Trends & Analysis **9**

The Psychology of Social Engineering: "Hot and Cold States of Mind" 9

About this Document

This report is prepared by the Bahá'í Internet Agency to assist individuals engaged with the protection of Bahá'í institutional assets either at the implementation level or at the level of planning and policy. These reports are intended for anyone associated with a Bahá'í institution, from professional IT staff to average users. Readers should scan the table of contents to see what is of interest to them. IT staff should feel free to take parts of these reports for distribution to their staff and to other institutions within their community.

The first section of this report provides excerpts from recent news stories, accompanied by the report editors' comments about the story, including relevance to Bahá'í institutional activity. The news section is followed by a focused discussion of a current or developing trend. The news section is intended to make readers aware of events they need to know about and perhaps take immediate action, and the Trends and Analysis section serves to create awareness of technologies or behaviors that may need to be considered in long-term plans.

This report comes in an audio form for those who would rather listen to it. At the end of the recording, the editors have a discussion about one of the report's main stories.

This month's recording topic is: **Dealing with panic.** (Discussion starts at: 16:49).

The website, Bahá'í IT Security Resources, contains all the educational and background materials generated by our Agency. This non-public website can be reached via https://sfa-resources.bic.org. The site is for those directly involved with supporting the IT operations of Bahá'í institutions. Although these resources provide information that is readily available online, we ask that the site link **not be shared with the public.** The site contains: current and past monthly security reports, Security Focus primers, podcasts, and the current Computer Security Manual for Bahá'í Institutions. Please note that the podcasts can be heard on your PC with the free "Music Player for Google Drive" browser extension. Mobile devices require the Google Drive app.

Many of our ideas for topics originate from IT staff and users in the field. The resource page includes a survey feedback form. Please let us know if you find the reports useful and which topics you would like to see covered in future issues.

Security News Digest

Lock down your Gmail account like it's Fort Knox with the Google Advanced Protection Program

Excerpted from: cNet

You store a ton of personal information in your Google account -- bank account balances, email addresses and phone numbers, pictures of your face, your friends' faces, your family. If you want to protect that sensitive data with the highest level of security you can get, consider the Google Advanced Protection Program. Google's program makes it nearly impossible for anyone other than you to access your Gmail, Google Drive, Google Photos or other Google services. Best of all, thanks to a recent update, adding what Google claims is the strongest level of consumer-grade security to your Google account just got a bit easier.

You have a reason to be concerned about your private information -- companies reported a staggering 5,183 data breaches in 2019 alone. And even though you may not be as high-profile of a target at Jeff Bezos, it's not particularly reassuring that even the CEO of one of the biggest tech companies on earth isn't impervious to getting his phone hacked. Sometimes even the effort to make your passwords as strong as possible isn't enough.

Editors' Note: This is an exceptionally secure means by which one can control access to one's personal Google account. The same system is included in the business version of Google, G Suite, but G Suite includes additional forms of protection, such a mobile device management system that provides extra protection to the users' phones. For individuals at high risk of being attacked, this APP system is well worth the effort required. And, because a security system is only as strong as the weakest part, telling people with whom your institutions collaborates on sensitive information about the advanced protection program could be in your institution's interest.

Iranian Phishers Use Journalist's Identity to Steal Info by Offering an Interview

*Excerpted from:*InfoSecurity

Security researchers have discovered a new phishing campaign from Iranian state-linked hackers which uses the lure of an interview with a noted journalist to trick recipients into clicking.

It's primarily designed to harvest email account info from journalists and political and human rights activists, as well as information about their contacts and networks.

The campaign is notable for spoofing the identity of a former Wall Street Journal writer, Farnaz Fassihi, to set up a non-existent interview with the recipient. However, the phishers made a glaring mistake: Fassihi is now at the New York Times, rendering the WSJ masthead on the email more than a little incongruous. The email also comes from a Gmail account.

Editors' Note: One of the favorite Iranian hacking methods is to pretend to be a journalist seeking an interview. Because the targets are the type of people to get interviewed, the request seems genuine. After the target believes that they are dealing with a legitimate journalist, the request to click on a link seems acceptable. This tactic has been used against Baha'is in the past and based on this recent report, we should expect this tactic to be used in the future. If you are contacted by a journalist, contact the journalist's organization to make sure you are actually in contact with their employee before engaging with the supposed journalist. The same would be true if the person claims to be an academic researcher or staff of an NGO.

Iranian hackers have been hacking VPN servers to plant backdoors in companies around the world

Excerpted from: ZDnet

2019 will be remembered as the year when major security bugs were disclosed in a large number of enterprise VPN servers, such as those sold by Pulse Secure, Palo Alto Networks, Fortinet, and Citrix.

A new report published today reveals that Iran's government-backed hacking units have made a top priority last year to exploit VPN bugs as soon as they became public in order to infiltrate and plant backdoors in companies all over the world.

According to a report from cyber-security firm ClearSky, Iranian hackers have targeted companies "from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors."

Editors' Note: We have to assume that the list of targets includes our institutions. Institutions using any VPN server should consult the vendor's site on protective measures. Even if your institution is not using VPN services, but VPN services are present, you should also check. Just because a service is not in use does not mean it cannot be accessed and exploited.

90% of UK Data Breaches Due to Human Error in 2019

Excerpted from: InfoSecurity

According to the cybersecurity awareness and data analysis firm [CybSafe], nine out of 10 of the 2376 cyber-breaches reported to the ICO last year were caused by mistakes made by end-users. This marked an increase from the previous two years, when respectively, 61% and 87% of cyber-breaches were ascribed to user error.

CybSafe cited phishing as the primary cause of breaches in 2019, accounting for 45% of all reports to the ICO. 'Unauthorized access' was the next most common cause of cyber-breaches in 2019, with reports relating to malware or ransomware, hardware/software misconfiguration and brute force password attacks also noted.

Oz Alashe, CEO of CybSafe, said: "As this analysis shows, it's almost always human error that enables attackers to access encrypted channels and sensitive information. Staff can make a variety of mistakes that put their company's data or systems at risk, often because they lack the knowledge or motivation to act securely, or simply because they accidentally slip up."

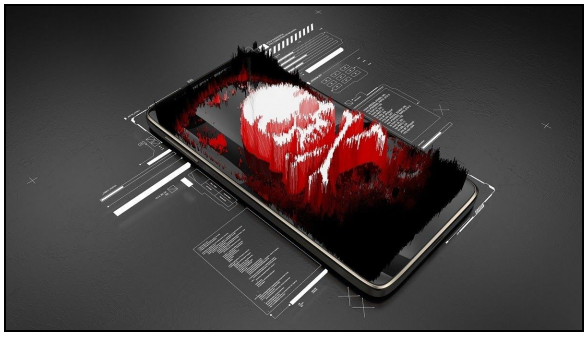
Editors' Note: The focus on security features often misses the main problem of user mistakes. As hardware and software systems improve, attackers shift to targeting the system's users. Let users know that they are part of the security system and that attackers will likely want to compromise the institution's systems via the users. A "Brute Force" attack is where the attacker guesses the user password simply by trying several hundred of the most common passwords that are easily downloaded from the Internet.

Bezos, WhatsApp Cyberattacks Show Growing Mobile Sophistication

Excerpted from: ThreatPost

Sophisticated nation-state groups are increasingly using mobile devices as an infection vector.

Oded Vanunu, head of products vulnerability research at Check Point research, told Threatpost during CPX 360 this week that because mobile devices come equipped with varying technologies, from communication apps to operating systems, they're ripe targets for sophisticated cybercriminals.



Recent examples of potentially state-sponsored mobile cyberattacks have included the reported hack of Jeff Bezos' phone, which reports say occurred after the Amazon CEO opened a seemingly benign WhatsApp video in 2018 from the account of the Saudi Crown Prince Mohammed bin Salman. More recently, New York Times journalist Ben Hubbard said this week that someone tried to hack his phone by sending him an Arabic text message with a link for a website. Beyond these high-profile instances, various journalists and human rights activists have been targeted globally after a WhatsApp zero-day vulnerability was exploited by attackers who were able to inject spyware onto victims' phones.

While it's certainly not the only way that mobile phones are being attacked, Facebook-owned WhatsApp has become a significant attack surface; it's used by 1.5 billion people globally, making it ripe for cybercriminals.

Editors' Note: The first major trend, as seen in the previous story, is a continued shift of attacks from hardware/software systems to the users. The second clear trend is the shift from attacks on large computer systems and PCs to attacks on mobile phones. Users need to use devices that are being kept updated by the vendors. Mobile devices should also have screen locks and some sort of antivirus

software. While this particular vulnerability has been patched by WhatsApp, clicking on a link received in an email or text message is almost never a good thing.

Also, it is a good idea to install one of several free anti-malware apps that can be a barrier between your mobile device and malicious content. Choices from reputable firms for antivirus software for mobile devices include Lookout, Sophos, Bitdefender, and McAfee Mobile Security. Most of these offer a paid version with more features, but often the free version is sufficient.

Microsoft Leaves 250M Customer Service Records Open to the Web

Excerpted from: ThreatPost

Misconfigured Microsoft cloud databases containing 14 years of customer support logs exposed 250 million records to the open internet for 25 days. The account info dates back as far as 2005 and is as recent as December 2019 — and exposes Microsoft customers to phishing and tech scams.

Microsoft said it is in the process of notifying affected customers.

The Comparitech security research team said that it ran across five Elasticsearch servers that had been indexed by search engine BinaryEdge, each with an identical copy of the database. The database contained a wealth of phishing- and scam-ready information in plain text, including: Customer email addresses, IP addresses and physical locations, descriptions of customer service claims and cases, case numbers, resolutions and remarks, and internal notes marked "confidential."

In short, it's everything a cybercriminal would need to mount a convincing and large-scale fraud effort, Comparitech researcher Paul Bischoff wrote in a posting on Wednesday.

"The data could be valuable to tech support scammers, in particular," he said. "Tech support scams entail a scammer contacting users and pretending to be a Microsoft support representative. These types of scams are quite prevalent, and even when scammers don't have any personal information about their targets, they often impersonate Microsoft staff. Microsoft Windows is, after all, the most popular operating system in the world."

Editors' Note: There are two primary reasons social engineering works. The first reason is that the attacker creates a sense of panic in the user. The second reason is that the attacker can include information that only the legitimate source of the message could possibly know. This recent exposure of Microsoft tech support information means that attackers will be able to send out highly convincing messages. Likely targets will be IT staff. Microsoft will be sending out notices to all the people potentially affected, but it's likely that most recipients of this message will likely think it's spam and delete it without reading it. Also, Microsoft never calls a user to tell them that their computer is infected, any calls of this nature are scams and need to be ignored and the number blocked for the future.

Microsoft says it now will continue to support Security Essentials for Windows 7

Excerpted from: MSFT

Microsoft has verified that it will continue to support Microsoft Security Essentials after seemingly contradictory information suggested that it won't be supported at all, even to those who purchased Extended Security updates for Windows 7.

Microsoft Security Essentials (MSE) will continue to receive signature updates after January 14, 2020.

Editors' Note: When Microsoft stopped support for Windows 7, the real problem for Windows 7 users – who comprise 38% of the current users – was security and not because of any lack of features. Exploits to take advantage of Win7 vulnerabilities found since Microsoft's drop-dead date of January 15th have already been discovered in active use. Microsoft says it will not fix any of the new vulnerabilities, but their recent decision to continue support for Security Essentials means that they will block access to the vulnerability. While we recommend moving off Windows 7, if there is a reason one must keep a Windows 7 PC, make sure it's still getting these security updates.

You can still get Windows 7 updates without paying a penny to Microsoft

Excerpted from: betaNews

0patch describes itself as "a microscopic solution for a huge security problem", issuing fixes for software faster than official developers, and it has pledged to continue to support Windows 7. Following on from what it did with Microsoft Office Equation Editor, 0patch has already announced that it is going to "security-adopt" Windows 7 and Windows Server 2008.

Microsoft has -- at least in theory -- released the last update for Windows 7 that will be available to everyone. So 0patch is taking over. The company will use security advisories that are issued by Microsoft to determine any vulnerabilities in Windows 7 and Windows Server 2008 that need addressing, and work to produce fixes.

Editors' Note: Opatch has recognized that there is a large number of owners with discontinued products. While Opatch cannot modify Microsoft's code, they can look at the updates Microsoft sells at great expense to corporate users who need to continue with Windows 7. Opatch then creates a small application that reproduces the behavior of the Microsoft patch. Of course, they do this for a far smaller amount of money than what Microsoft requires. And, fortunately for us, their patches are free for nonprofits and home users. Microsoft does not have a similar program for these users because their business model is to move everyone possible to Windows 10. Opatch benefits from users staying on Windows 7; Microsoft doesn't.

Trends & Analysis

The Psychology of Social Engineering: "Hot and Cold States of Mind"

Psychology recognizes that when people get into a "hot state", represented by a high level of emotion, the logical processes of the mind in a "cold state" are often forgotten. Social engineers use this aspect of human nature to bypass the target's logical process. Attackers don't want their targets to think, "why am I getting this message?", "the policy is to contact the sender via another communication channel", "perhaps I should contact our IT person to see if this is legitimate". Most people who fell victim to social engineering report that "something wasn't right" or they "knew something wasn't right", etc. Yet they took action prompted by the attacker.

It would be incorrect to assume that social engineering attacks only work with inexperienced or foolish people. Nothing could be further from the truth. Social engineering works with security professionals, staff of security agencies, and with people who have been successfully attacked in the past. The problem is that logic and experience do not work when a person is in an emotional state. While not all social engineering involves eliciting emotional reactions, many do. Messages of "your account has been hacked and we need to confirm you're the rightful owner" or "your new car purchase has been approved for financing", try to create panic in the recipient such that all the logical precautions they know well are forgotten or discounted.

The question for security minded people is how to counter the "hot states" when training and logic are the first victims of such a state of mind? Training helps to some extent, knowing who to call if there is a problem might prevent an action being taken before it is too late. Having people in the environment knowing what to do can help. Presumably, they are better able to think clearly.

Perhaps one of the best steps is to inform possible targets of social engineering attacks, that if some message or call has caused a strong emotional response that emotional response should be considered a security warning.